Lapinlahden kunnan hallinnon tietoturvasuunnitelma

Auli Turunen

Opinnäytetyö

___. ___. _____ _____

Ammattikorkeakoulututkinto

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Auli Turunen	
Työn nimi Lapinlahden kunnan hallinnon tietoturvasuunnitelma	
Päiväys 25.11.2011	Sivumäärä/Liitteet 28 + 22
Ohjaaja(t) Lehtori Kalevi Kolehmainen, hallintojohtaja Matti Sollo	
Toimeksiantaja/Yhteistyökumppani(t) Lapinlahden kunta	

Tiivistelmä

Jokaisen organisaation velvollisuus on järjestää oman toimintansa tietoturva noudattamalla lainsäädännössä tietoturvasta annettuja ohjeita ja määräyksiä. Kuntien tietoturvan kehittämiseen ja laadintaan tarvittavaa tarkkaa ohjeistusta tai mallia ei ole vielä saatavilla. Valtiovarainministeriön laatimia valtionhallinnon käyttöön tarkoitettuja ohjeita ja suosituksia voidaan kuitenkin soveltaa myös kuntien tietoturvaa kehitettäessä.

Tämän insinöörityön tarkoituksena oli suunnitella ja laatia Lapinlahden kunnan hallinnon tietoturvasuunnitelma. Työssä perehdytään tietoturvan käsitteistöön, kuvataan tietoriskejä, tutustutaan riskienhallintaan ja keskeisimpiin julkishallinnon tietoturvaa koskeviin lakeihin. Kunnan tietoturvasuunnitelmassa esitellään kunnan virasto-organisaatiota hallintokeskuksen näkökulmasta. Suunnitelmassa kartoitetaan tietoturvan nykytila ja käydään läpi tietohallintariskejä, toimintatapoja sekä keinoja riskien vähentämiseksi ja pienentämiseksi.

Työn tuloksena valmistunutta kunnan ensimmäistä tietoturvasuunnitelmaa voidaan pitää jatkossa toteutettavan kehittämissuunnitelman apuvälineenä.

Avainsanat
tietoturva, riskienhallinta, tietoturvasuunnitelma

julkinen

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Auli Turunen			
Title of Thesis The information security plan for Lapinlahti municipality			
Date	2011-11-25	Pages/Appendices	28 + 22
Supervisor(s) Mr. Kalevi Kolehmainen, Lecturer, Mr. Matti Sollo, Director of Administration			
Client Organisation/Partners Lapinlahti municipality			

Abstract

Every organization has a responsibility to manage their own information security according to instructions and orders included in the law. There is no ready template to be used in designing and improving information security of municipalities. Government's instructions and recommendations made by ministry of finance can be adapted to use in improving information security of municipalities.

This thesis was meant to design an information security plan for Lapinlahti municipality. This thesis includes orientation with terms and risks of information security, risk management and crucial parts of government information security legislation. The information security plan for Lapinlahti municipality presents the organization from the perspective of IT management. The plan shows the current state of information security and lists management risks, policies and different ways to decrease the risks.

The result of this thesis is the first version of the information security plan of Lapinlahti municipality. The plan can be used as a basis for the improvement plan that is yet to come.

Keywords
information security, risk management, information security plan

public

ALKUSANAT

Tämä opinnäytetyö on tehty Lapinlahden kunnalle. Haluan kiittää työn ohjaajaa Matti Solloa Lapinlahden kunnasta ja ohjaavaa opettajaa lehtori Kalevi Kolehmaista Savonia-ammattikorkeakoulusta saamistani neuvoista ja ohjauksesta.

Erityisesti haluan kiittää perhettäni saamastani taustatuesta ja kannustuksesta koko opiskeluni aikana.

Lapinlahti 17.5.2012

Auli Turunen

SISÄLTÖ

TERMIT JA LYHENTEET

Lyhenne	Kuvaus
Riskienhallinta	Järjestelmällinen tutkimus kaikista tietyn kohteen riskeistä ja niiden suuruudesta sekä tähän perustuva riskienhallintakeinojen valitseminen ja käyttäminen.
Tietoturva; tietoturvallisuus	Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.
Tietoturvapolitiikka	Organisaation hyväksymä näkemys organisaation tietoturvan päämääristä, periaatteista ja toteutuksesta.
Tietoturvariski	Tietoturvauhan toteutumisen todennäköisyys ja mahdollisesti toteutuvan vahingon merkittävyys.
Tietoturvastrategia	Strategia tietoturvapolitiikan ja –periaatteiden jalkauttamiseksi.
Tietoturvasuunnitelma (Tietoturvallisuuden kehittämissuunnitelma)	Riskianalyysiin perustuva tietoturvallisuuden arvioinnin tulos, joka on perusta tulevalle kehittämistyölle. Kehittämissuunnitelma toimii toteutuksen ohjaajana toimenpiteille, joilla korjataan tietoturvallisuuden arvioinnissa havaitut puutteet ja joiden avulla pyritään hallitusti kehittämään tietoturvallisuuden kypsyystasoa tavoitetasolle.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriön asettama ja johtama hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elin.

1 JOHDANTO

Julkishallinnossa käsitellään paljon tärkeää tietoa ja toiminta on nykyään erittäin suuressa määrin riippuvainen tietotekniikasta. Useat toiminnot ja palvelut hoidetaan tietoverkkojen kautta, joten niiden tietoturvallisuudesta huolehtiminen on tärkeää. Tietoturvallisuudesta puhuttaessa yhdistetään asiat usein tekniseen turvallisuuteen, mutta ihmisenkään roolia ei pidä unohtaa. Monet tietoturvan aukot ovat syntyneet ihmisten tekemistä tahattomista tai tahallisista rikkeistä. Salassa pidettäviä, arkaluontoisia ja luottamuksellisia tietoja tulisikin suojata niin, etteivät ne joudu millään tavalla asiattomien käsiin. Jokaisen organisaation velvollisuus on huolehtia oman toimintansa tietoturvallisuuden järjestämisestä noudattamalla lainsäädännön tietoturvasta antamia ohjeita ja velvoitteita.

Tämän työn aiheena on tietoturvasuunnitelman laatiminen Lapinlahden kunnan hallinnolle. Kunnalla ei ole ollut aikaisemmin varsinaista tietoturvasuunnitelmaa, vaan ohjeistusta on ollut saatavilla erilaisten yksittäisten ohjeiden ja oppaiden muodossa. Kunnan tietotekniikkapalvelut on ulkoistettu. Palvelujen tuottamisesta vastaa Fujitsu Finland Oy. Kunnan tietotekniikasta vastaa tällä hetkellä hallintojohtaja Matti Sollo.

Testasin kunnan työntekijöitä tietoturvan perustason testillä (liite 1). Testiin kuului 20 kysymystä tietoturvallisuudesta. Lähetin testin 20 henkilölle ja sain vastaukset 14 henkilöltä. Eniten virheellisiä vastauksia löytyi tietoaineiston tietoturvallisesta käsittelystä, salassa pidettävien asiakirjojen luokittelusta, etäkäytöstä ja etätyöstä sekä muun sähköpostijärjestelmän kuin virkasähköpostin käyttämisestä omassa työssä.

Opinnäytetyön alussa luvussa 2 käydään läpi tietoturvallisuutta yleisesti, tutustutaan tietoturvallisuuden vaatimuksiin ja osa-alueisiin. Luvussa 3 keskitytään tietoriskeihin ja riskienhallinnan prosessiin. Luvussa 4 tutustutaan keskeisimpiin julkishallinnon tietoturvaan liittyviin lakeihin. Luku 5 käsittelee tietoturvaa kunnallishallinnossa. Lopuksi luvussa 6 pohditaan opinnäytetyön toteuttamiseen liittyviä ratkaisuja sekä luodaan yleiskatsaus Lapinlahden kunnan hallinnon tietoturvasuunnitelmaan.

2 TIETOTURVALLISUUDEN KÄSITTEET

2.1 Tietoturvallisuus

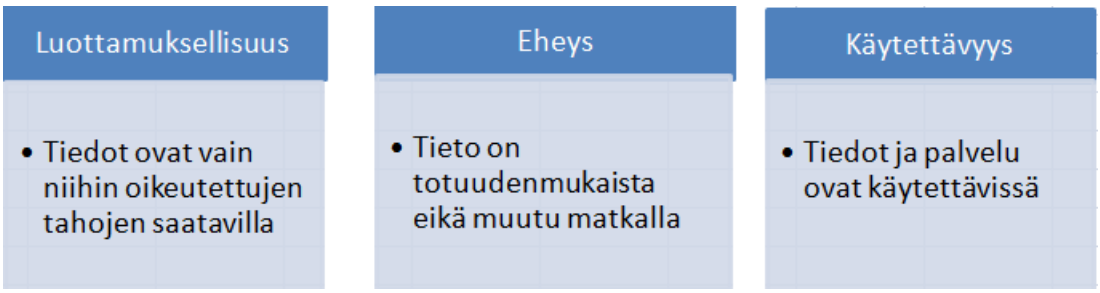
Tietoturvallisuudella pyritään vaikuttamaan tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen. Salaisen tiedon päätyminen henkilölle, joka ei ole siihen oikeutettu, voi aiheuttaa vahinkoa yritykselle ja sen imagolle. Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. (VAHTI 5/2003, 8). Laitteisto- ja ohjelmistoviat, tapaturmat tai luonnontapahtumat ovat huomioonotettavia uhkia yrityksen toiminnalle, joten näiden tekijöiden tietoturvallisuuteen tulee suhtautua vakavasti.

2.2 Tietoturvallisuuden vaatimukset

Tietoturvallisuuden perusominaisuudet voidaan jakaa CIA-mallin mukaan kolmeen osaan, jotka koostuvat luottamuksellisuudesta (Confidentiality), eheydestä (Integrity) ja käytettävyydestä (Availability).

Näiden lisäksi tähän joukkoon lisätään nykyään todentaminen (Authentication), mikä tarkoittaa luotettavaa tunnistamista ja kiistämättömyys (Non-repudiation), joka tarkoittaa, ettei tapahtumaa voi kiistää jälkikäteen.

CIA-mallin mukaiset keskeiset käsitteet ovat alla olevassa kuvassa (kuva1).



Kuva 1. CIA-malli tietoturvallisuuden vaatimuksista

Luottamuksellisuudella tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.

Eheydellä tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

Käytettävyydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niiden käyttöön oikeutettujen esteettä hyödynnettävissä. (Viestintävirasto)

2.3 Tietoturvallisuuden osa-alueet

Tietoturvallisuus voidaan jakaa osa-alueisiin, jotka saumattomasti kaikki yhdessä hoidettuna takaavat sen, että tietoturva on kunnossa. Osa-alueet muodostuvat seuraavista tekijöistä:

2.3.1 Hallinnollinen tietoturvallisuus (administrative information security)

Hallinnollinen tietoturvallisuus pitää sisällään yrityksen tietoturvallisuuspolitiikan, toimintalinjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyt, tietoturvallisuuteen tähtäävän ohjeistuksen, koulutuksen ja valvonnan.

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohjeessa tietoturvapolitiikkaa kuvataan seuraavasti:

Tietoturvapolitiikan avulla johto määrittelee tietoturvatoiminnan tavoitteet, vastuut ja toimintalinjaukset. Tietoturvallisuuden merkityksen ja tietoturvatyön yleisperiaatteiden määrittely, dokumentointi ja viestintä jokaiselle organisaation työntekijälle on välttämätön perusta tietoturvakulttuurin luomiselle. Tietoturvapolitiikka toimii perustana, jonka varaan erilaiset tietoturvasuunnitelmat ja –ohjeistukset rakentuvat.
Tietoturvapolitiikan luomista ohjaavat organisaation toiminnan tarkoitus ja strategia, riskianalyysi, lait ja määräykset. (VAHTI X/2007, 18, 19)

2.3.2 Henkilöstöturvallisuus (personnel security)

Henkilöstöturvallisuus on henkilöstöstä johtuvaa riskien hallintaa. Sen perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvavastuut ja – tehtävät on selkeästi kuvattu toimenkuvissa. Lisäksi tarvitaan riittävällä tasolla määriteltynä olevat henkilöstöhallinnon prosessit sekä muut prosessit, joissa kuvataan työtehtävät niin tarkasti, että avainhenkilöriskien syntyminen vältetään. Keskeisiä asioita ovat työhönottoon, toimenkuvien olennaisiin muutoksiin ja palvelussuhteen loppumiseen liittyvät proses-

sit ja niistä on tarpeen olla kaikilla osallisilla käytössään sovittu toimintamalli. (Kunnat.net – Tietoturva)

2.3.3 Fyysinen turvallisuus (physical and environmental security)

Tähän tietoturvallisuuden osa-alueeseen kuuluvat muun muassa kulunvalvonta, kameravalvonta, muu tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta. Vähimmäisvaatimukset tilaturvallisuutta lisääville toimille ja järjestelmille määräytyvät turvallisuustarpeiden perusteella, jotka voi kohdistua alueeseen, rakennukseen, tilaryhmään tai tilaan. (Kunnat.net – Tietoturva)

2.3.4 Laitteistoturvallisuus (computer security)

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. Laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon kuuluvat myös asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja - sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa. (Kunnat.net – Tietoturva)

2.3.5 Tietoliikenneturvallisuus (telecommunications security)

Organisaation tietoliikennetoiminnot ja niitä toteuttavat eri verkkojärjestelmät suunnitellaan ja rakennetaan hyvän tiedonhallintatavan mukaisesti siten, että valittu arkkitehtuuri tukee varautumista erilaisia uhkia vastaan. Tietoliikenneturvallisuuteen sisältyvät muun muassa tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, merkittävien tietoturvapoikkeamien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. (Kunnat.net – Tietoturva)

2.3.6 Ohjelmistoturvallisuus (software security)

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistamis-, suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. Ohjelmistojen turvallisuuteen vaikuttavat ohjelmistokehitykses-

sä käytetyt prosessit, ohjelmiston käytönaikaiset asetukset ja ohjelmiston palvelualustan (käyttöjärjestelmän ja mahdollisten väli- ja apuohjelmistojen) asetukset sekä käyttäjien saama koulutus ja ohjeistus. (Kunnat.net – Tietoturva)

2.3.7 Tietoaineistoturvallisuus (data information security)

Tietoaineistoturvallisuudessa on kyse eri talletusmuodoissa olevien tietojen suojauksesta. Se koskee paperiasiakirjoja, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä sekä muita vastaavia teknisiä laitteita. Tietoaineistoturvallisuus kattaa käsittelysäännöt tietoaineiston synnystä sen tuhoamiseen asti. (Kunnat.net – Tietoturva)

2.3.8 Käyttöturvallisuus (operations security)

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet. Tämä toteutetaan huolehtimalla muun muassa toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. Kaikkien tietojärjestelmien suojaaminen haittaohjelmilta (kuten sähköpostiviruksilta tai verkkomadoilta) on osa käyttöturvallisuutta. Järjestelmien käyttöturvallisuuden taso perustuu järjestelmässä olevien tietojen luokitukseen. (Kunnat.net – Tietoturva)

3 TIETORISKIT

Tietoturvallisuus ja tietoturvariskien hallinta on osa yrityksen johtamistoimintaa. Useat lait ja asetukset kuten esimerkiksi Laki viranomaisen toiminnan julkisuudesta (621/1999), asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), Henkilötietolaki (523/1999) ja Valmiuslaki (1080/1991) sisältävät velvoitteita tietoturvariskejä arvioitaessa.

Jos riskejä ei tunnisteta, ei niitä voida hallitakaan. Riskien aiheuttajina saattavat olla tekniset, luonnonilmiöistä aiheutuvat tai ihmisen tahallaan tai tahattomasti aiheuttamat viat. Yrityksen verkkoon tunkeutuminen, tiedonsiirtoon liittyvät väärinkäytökset, virukset, madot, salasanojen joutuminen vääriin käsiin, vesivahingot, tulipalot, sähköhäiriöt sekä laitteisto- ja ohjelmistoviat voivat muun muassa uhata toiminnan jatkuvuutta. Riskeihin tulee aina varautua niin, että tiedon luottamuksellisuus, käytettävyys ja eheys turvataan.

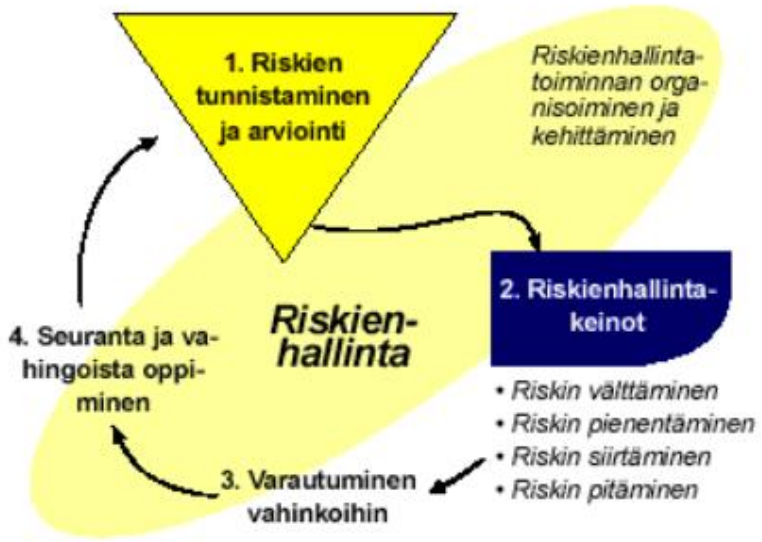
Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTi on julkaissut riskien arvioinnista tietoturvallisuuden edistämiseksi seuraavan kannanoton:
Tietoturvallisuuden perusta on tunnistaa ja arvioida organisaation toimintaan liittyvät tietoriskit. Tämän pohjalta voidaan tehdä päätökset siitä, mitä toimenpiteitä pitää toteuttaa. Riskejä hallittaessa lähtökohdaksi on otettava organisaation toiminnan kehittäminen, kuten esimerkiksi toimintatavat, osaaminen ja johtaminen. Sen jälkeen tulevat tekniset suojauskeinot.

Johdon tulee voida perustaa tietoturvapolitiikkaa ja – periaatteita koskevat päätökset riskianalyysin osoittamiin tarpeisiin. Samoin tietoturvallisuutta koskevat yksityiskohtaiset suunnitelmat perustuvat riskianalyysin tuloksiin. (VAHTI 7/2003)

3.1 Riskienhallinta

Riskienhallinnalla on selkeät päävaiheet. Ensin riskit on tunnistettava ja arvioitava. Sen jälkeen suunnitellaan riskien torjunta ja tarvittavat toimenpiteet. Kolmannessa vaiheessa suunnitellaan, miten vahingon sattuessa toimitaan ja miten vahingoista toivutaan. Viimeisessä vaiheessa tilannetta seurataan. Parhaassa tapauksessa vahingosta myös opitaan. (pk-rh.fi - Riskienhallintaprosessin vaiheet)

Riskienhallinnanprosessin eteneminen vaiheittain on esitetty kuvassa 2.



Kuva 2. Riskienhallintaprosessi. (pk-rh.fi – Riskienhallintaprosessin vaiheet)

3.2 Riskien tunnistaminen ja arviointi

Riskien arvioinnissa tulee tunnistaa organisaation toiminnalle tärkeät kohteet, joiden suojaaminen on ensiarvoisen tärkeää toiminnan jatkuvuudelle. Esimerkiksi tietojärjestelmät, sovellukset, tietoliikenneyhteydet, konesalit, arkistot, asiakastilat ja toimistotilat ovat tärkeitä suojaamisen kohteita.

Riskin suuruuteen vaikuttavat mahdollisten seurausten vakavuus ja todennäköisyys. Tärkeää on tunnistaa ne isoimmat riskit, jotka kiireisimmin vaativat ratkaisua. Tämän vuoksi määritellään ensin riskin suuruus arvioimalla uhkan seurauksena mahdollisesti syntyvien vahinkojen suuruus ja vahingon todennäköisyys. (VAHTI 7/2003, 41)

Riskitaulukossa (taulukko 2) uhkan todennäköisyys on luokiteltu 0 – 3 asteikolla. Uhkan todennäköisyys on korkea arvolla 3, keskimääräinen arvolla 2 ja alhainen arvolla 1. Vastaavasti seurausten vakavuus on määritelty asteikolla 0 – 3, jossa seurausten vakavuus on erittäin vakava arvolla 3, vakava arvolla 2 ja vähäinen arvolla 1. Kun uhkan todennäköisyys on alhainen (1) ja seurausten vakavuus on vähäinen (1), on kyseessä merkityksetön riski (1) ja vastaavasti uhkan todennäköisyyden ollessa korkea (3) ja seurausten vakavuuden erittäin vakava (3), on kyseessä sietämätön riski (5).

Taulukko 2. Riskitaulukko (VAHTI 7/2003, 43)

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1.Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Taulukon 3 esimerkissä selitetään uhkan todennäköisyyttä luokittelun eri kohdissa. Taulukosta selviää se tosiasia, että uhkan todennäköisyys on alhainen silloin, kun toiminta on hyvin valvottua ja toimintoihin pääsy on hallittua.

Taulukko 3. Esimerkki uhkan todennäköisyyden arvioinnin asteikosta (VAHTI 7/2003, 41)

Korkea	**3**	• Toiminto tai järjestelmä on heikosti valvottua • Toimintoon tai järjestelmään pääsy on helppoa • Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa • Toiminnon ohjeistusta ei ole • Tapahtuma ilmenee kerran kuukaudessa • Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä (oma henkilöstö, yhteistyökumppanit, ulkopuoliset)
Keskimääräinen	**2**	• Toiminto on osittain valvottua • Toiminnon ohjeistus on puutteellista • Tapahtuma ilmenee 1–2 kertaa vuodessa • Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille (atk-tuki)
Alhainen	**1**	• Toiminto on hyvin valvottua ja siihen pääsy on hallittua. • Toiminto on hyvin ohjeistettu • Toimintoa kohtaan ei ole mielenkiintoa • Tapahtuma ilmenee kerran vuodessa • Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille (asiantuntijat)
Ei merkitystä	**0**	• Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

Taulukosta 3 voidaan todeta myös se, että uhkan todennäköisyys on alhainen toiminnon ollessa hyvin ohjeistettu ja toimintoon ei liity erityistä mielenkiintoa. Uhka ilmenee kerran vuodessa ja sen toteuttaminen on mahdollista vain yksittäisille työntekijöille. Tarkasteltaessa tilannetta silloin, kun uhkan todennäköisyys on korkea, huomataan kaikkien toimintojen olevan päinvastaisia kuin uhkan todennäköisyyden ollessa alhainen.

Seuraavasta taulukosta (taulukko 4) voidaan tarkastella valtiovarainministeriön laatiman esimerkin avulla seurausten vakavuuden luokittelua.

Taulukko 4. Esimerkki seurausten vakavuuden luokittelusta (VAHTI 7/2003, 42)

Erittäin vakavat	**3**	• Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä • Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille • Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin • Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia • Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) • Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen • Toiminta on lainsäädännön velvoitteiden vastaista.
Vakavat	**2**	• Seurauksilla on vaikutuksia organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys) • Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä • Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) • Uhkan toteutuminen aiheuttaa tiedotteen tekemisen • Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
Vähäiset	**1**	• Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä • Uhkan toteutuminen aiheuttaa sisäisen raportoinnin • Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia • Toiminnan keskeytyminen on muutaman minuutin pituinen

Riskien arvioinnin dokumentointiin on valtiovarainministeriö laatinut kuvan 3 mukaisen mallin. Mallin mukaan jokaiselle riskille annetaan sitä hyvin kuvaava nimi, kirjataan riskin tavoitteet, selvitetään syyt riskin olemassaoloon ja tehdään tarvittavat toimenpiteet riskin poistamiseksi tai ennaltaehkäisemiseksi. Lopuksi laaditaan aikataulu toimenpiteiden korjaamiseksi ja nimetään vastuuhenkilö, joka huolehtii annetuista tehtävistä.

Riski	**Internet palvelimen tietoturvariski (murto)**
Tavoite	Tavoitteena on sekä riskin todennäköisyyden että seurausten vakavuuden pienentäminen.
Syy riskin olemassaoloon	Käyttöjärjestelmän suunnittelussa on unohdettu riittävästi huomioida tietoturvallisuuteen liittyviä tekijöitä tai toiminnallisuuden takaamiseksi on turvaominaisuuksista osittain luovuttu. Testauksessa ei ole löydetty kaikkia aukkoja joita hyökkääjä voi hyödyntää.
Toimenpide-ehdotus	Toimintaympäristön tapahtumia seurataan. Palvelimen ohjelmisto päivitetään usein. Hankitaan seurantatyövälineitä joilla mahdollinen murto voidaan havaita.
Aikataulu ja vastuuhenkilö	Toiminnan seuranta on jatkuvaa. Hankitaan tarvittavat ohjelmistot kahden kuukauden aikana. Vastuuhenkilö on MM

Kuva 3. Esimerkki yhden riskin hallintasuunnitelma (VAHTI 7/2003, 47)

3.3 Riskienhallintakeinot

Kun toiminnan uhkat on saatu tunnistettua ja niiden toteutumisen todennäköisyys ja seurausten vakavuus arvioitua, suunnitellaan ja päätetään toimenpiteistä, miten riskejä pyritään hallitsemaan. Keskeisimpinä toimintavaihtoehtoina ovat riskin välttäminen, riskin poistaminen, riskin pienentäminen, riskin siirtäminen, ja riskin pitäminen omalla vastuulla. (VAHTI 7/2003, 21)

Tarvittavat toimenpiteet riippuvat aina riskien suuruudesta. Pääsääntöisesti suurimpien riskien poistaminen tai pienentäminen kuuluu etupäässä tehtäviin toimenpiteisiin. Listaamalla tarvittavat toimenpiteet esimerkiksi taulukkoon, ymmärretään, miten tulee menetellä, kun riski on merkityksetön, vähäinen, kohtalainen, merkittävä tai sietämätön.

3.4 Riskien seuranta

Valtiovarainministeriön laatimassa ohjeistuksessa (VAHTI 7/2003, 47) kerrotaan, mistä asioista tulee sopia, kun riskien arvioinnin tuloksena laadittuja toimenpide-ehdotuksia ruvetaan toteuttamaan ja viemään eteenpäin. Samalla sovitaan asioiden hoidolle vastuuhenkilöt ja karkea aikataulu.

Tarkastelun tulokset pitää saattaa asianomaisten tietoon. Tuloksista tulee tiedottaa sekä viraston johtoa että kohteen henkilöstöä ja kertoa jatkotoimenpiteistä. Tiedottaminen voidaan hoitaa organisaation normaalin tiedotuskäytännön mukaisesti järjestämällä tiedotustilaisuuksia, tiedottamalla asiasta sopivissa kokouksissa, julkaisemalla keskeiset tulokset esimerkiksi henkilökuntalehdessä tai laatimalla erillinen tiedote. (VAHTI 7/2003, 48)

4 LAINSÄÄDÄNTÖ JA TIETOTURVALLISUUS

Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä. Tietoturvaan liittyviä säännöksiä löytyy useista laeista ja asetuksista. Keskeisimpiä julkishallinnon tietoturvatoimintaan liittyviä lakeja ovat muun muassa seuraavat, jotka käyn hieman tarkemmin läpi niin, että kunkin lainpykälän sisältö tarkentuu. Jokaisen lain kohdalla on erikseen viite siitä, mistä voi käydä tutustumassa lakiin tarkemmin.

Suomen perustuslaki (731/1999) (2. luku 10 § Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)

Jokaisen henkilön perusoikeus on oikeus yksityiselämään ja sen suojaan. Toiselle henkilölle osoitettua tekstiviestiä tai sähköpostiviestiä ei saa lukea. Esimerkiksi työnantaja ei missään olosuhteissa saa lukea työntekijöiden sähköposteja. Samoin työntekijän terveyttä koskevat asiat, esim. tupakointi, kuuluvat vain työntekijälle ja työterveyshuollolle, eivät työnantajalle.

Suomen perustuslaki (731/1999) (2. luku 12 § Viranomaisen hallussa olevien asiakirjojen ja tallenteiden julkisuus)

Jokaisella yksilöllä on sananvapausoikeus. Jokaisella on myös oikeus vaikuttaa yhteisiin asioihin. Tämän vuoksi henkilö on oikeutettu saamaan luotettavaa tietoa viranomaisten toiminnasta ja sen vaikutuksesta.

Kunnat tiedottavat ilmoitustaululla tai internetin kautta toimintaansa liittyvistä julkisista asioista. Monen kunnan kotisivuilla on mahdollisuus tutustua kunnan tekemiin päätöksiin eri toimielinten pöytäkirjojen välityksellä. Tämä edellyttää sitä, että aineistot ja asiakirjat on laadittu julkisuusperiaatteita noudattaen ja tietojärjestelmät toimivat hyvin. Halutessaan voi yksityishenkilö käydä kuuntelemassa esimerkiksi kunnanvaltuuston kokousta.

Suomen perustuslaki 11.6.1999/731
http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Lakia viranomaisen hallussa olevien asiakirjojen ja tallenteiden julkisuudesta koskeva sisältö on osin sama kuin laki viranomaisten toiminnan julkisuudesta.

Laki viranomaisten toiminnan julkisuudesta (18 § Hyvä tiedonhallintatapa)

Viranomaisen hyvästä tiedonhallintatavasta sanotaan, että viranomaisen tulee huolehtia, että asiakirjat ja tietojärjestelmät sekä niihin liittyvät tiedot ovat asianmukaisesti saatavilla, käytettävissä ja suojattuja. Lisäksi tulee ottaa huomioon muut tietojen laatuun vaikuttavat tekijät.
Esimerkiksi erilaiset kunnan toimielinten pöytäkirjat löytyvät internetistä kunnan internetsivuilta. Tiedot siirtyvät kokouksista pöytäkirjoihin muuttumattomina, eikä niiden sisältö muutu internetiin siirrettäessäkään.

Laki viranomaisten toiminnan julkisuudesta (24 § Salassa pidettävät viranomaisen asiakirjat)

Laki viranomaisten toiminnan julkisuudesta (621/1999) 24 § nimeää ne viranomaisen asiakirjat, jotka ovat salassa pidettäviä, jollei muuta ole säädetty. Asiakirjana pidetään perinteisessä muodossa olevaa paperidokumenttia tai se voi olla tietojärjestelmässä oleva elektroninen tieto. Asiakirjat ryhmitellään laissa 32 eri ryhmään niiden asiasisällön tai käyttötarkoituksen mukaan. Esimerkkeinä voidaan mainita salassa pidettävät henkilötiedot sekä liike- ja ammattisalaisuudet. Myös yhteiskunnan turvallisuuden tai tiettyjen keskeisten etujen vuoksi arkaluonteiset tiedot kuuluvat näihin.

Laki viranomaisten toiminnan julkisuudesta (621/1999 18 § ja 24 §)
http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Henkilötietolaki (523/1999) (3 § Henkilötietojen käsittelyä koskevat yleiset periaatteet)

Henkilötietolaki (523/1999) on henkilötietojen käsittelyn peruslaki (yleislaki). Henkilötietoja voidaan muun muassa kerätä ja tallettaa erilaisiin rekistereihin, esimerkiksi Effica-kotihoidon rekisteriin. Rekistereitä muodostuu esimerkiksi asiakassuhteen luomisen tai jäseneksi rekisteröitymisen yhteydessä asiakkaasta tallennetuista henkilötiedoista. Henkilön on annettava suostumuksensa tietojensa käsittelyyn ja tietoja saa käyttää vain siihen tarkoitukseen, mihin rekisteri on perustettu.

Henkilötietolaki (523/1999) (32 § Tietojen suojaaminen)

Henkilötietojen käsittelyyn voivat osallistua vain ne henkilöt, joilla on siihen käyttöoikeudet. Omia käyttäjätunnuksia ja salasanoja ei saa antaa ulkopuolisille, edes samaa

rekisteriä käsitteleville henkilöille. Henkilötietojen käsittelijät on perehdytettävä omaan työhön liittyviin tietoturvakäytäntöihin. Tietosuojaa pyritään turvaamaan, esimerkiksi terveystietojen osalta, seuraamalla lokitietoja, joista selviää luvatta asialla liikkuneet henkilöt.

Henkilötietolaki 22.4.1999/523 http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Rikoslaki (19.12.1889/39) (34. luku, 9a§ Vaaran aiheuttaminen tietojenkäsittelylle ja 38. luku 8§ Tietomurto)

Rikoslaissa säädetään tietoturvarikoksista ja niiden rangaistuksista. Rikoslain 34. luvun 9a pykälä koskee vaaran aiheuttamista tietojenkäsittelylle ja 38. luvun 8 pykälä tietomurtoja. Tuomiot vaihtelevat teon vakavuudesta johtuen sakkorangaistuksista jopa vankeuteen.
Vaaran aiheuttaminen tietojenkäsittelylle tarkoittaa, ettei esimerkiksi omalle työkoneelle saa asentaa ylimääräisiä ohjelmia tai laitteita. Tietomurto-kohta koskee käyttäjätunnuksen väärinkäyttöä. Jos joku varastoi tai siirtää tietoa hänelle kuulumattomalla käyttäjätunnuksella, syyllistyy hän tietomurtoon. Myös tietomurron yritys on rangaistava teko.

Rikoslaki 19.12.1889/39 http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Valmiuslaki 1080/1991 (Luku 6 40 § Varautuminen)

Valmiuslaissa säädetään valtioneuvoston, valtion hallintoviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien valmiussuunnitelmista sekä poikkeusoloissa tapahtuvasta toiminnan järjestelystä etukäteisvalmisteluin sekä muilla toimenpiteillä varmistetusta tehtävien mahdollisimman häiriöttömästä hoitamisesta. Esimerkiksi sodan syttyessä tietojärjestelmien häiriötön toiminta on taattava riittävillä varotoimenpiteillä. Kouluttautuminen tällaista tilannetta varten on tärkeää ja siihen on hyvä olla valittuna tietyt vastuuhenkilöt.

Valmiuslaki 1080/1991, Luku 6 40 § http://www.finlex.fi/fi/laki/alkup/1991/19911080

Arkistolaki (831/1994) (luku 4 11 § ja 12 § Asiakirjojen laatiminen, säilyttäminen ja käyttö)

Arkistolain (831/1994) 4. luvussa pykälissä 11 ja 12 on ohjeistus siihen, miten pysyvät asiakirjat, kuten 18.–20. päivä syntyneiden asiakirjat, on tallennettava ja säilytettävä. Asiakirjojen materiaalien ja säilyvyyttä turvaavien menetelmien on oltava arkistolaitoksen ohjeiden mukaisia.

Asiakirjoja on säilytettävä niin, että ne eivät ole vaarassa tuhoutua eikä niitä voi vahingoittaa tai käyttää asiattomasti. Myös arkistointiin tarkoitettujen tilojen on oltava arkistolaitoksen määräysten mukaiset.

Arkistolaki (831/1994) http://www.finlex.fi/fi/laki/ajantasa/1994/19940831

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) (luku 2, 4 §)

Laissa yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta luvussa 2 pykälässä 4 sanotaan, että jos televiestintää ei ole erityisesti tarkoitettu yleisesti vastaanotettavaksi, on se luottamuksellista. Jos joku ottaa vastaan luottamukselliseksi tarkoitettua televiestintää, hän ei saa ilmaista sen sisältöä tai kertoa sen olemassaolosta.
Esimerkiksi puhelinkeskustelun tahaton kuuleminen rikkoo luottamuksellisuuden, eikä puhelun vahingossa kuullut henkilö saa millään tavalla ilmaista, että on sen kuullut saati levittää siitä tietoa.

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) http://www.finlex.fi/fi/laki/alkup/1999/19990565

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) (1. luku, 1 §)

Laissa sähköisestä asioinnista viranomaistoiminnassa (13/2003) ensimmäisessä luvussa ensimmäisessä pykälässä on maininta, miten edistämällä sähköisten tiedonsiirtomenetelmien käytöllä on tarkoitus saada asiointi sujumaan helposti ja nopeasti. Sähköisen asioinnin tarkoitus on lisätä myös tietoturvallisuutta.

Esimerkiksi virkahakemukset voidaan lähettää sähköpostitse tavallisen kirjeen sijaan. Lisäksi erilaiset sähköiset lomakkeet on helpompi ja nopeampi täyttää sähköiseen lomakepohjaan. Koska sähköiset lomakkeet toimivat suojatussa yhteydessä, ne ovat tietoturvaltaan tavallista kirjettä parempia.

Laki sähköisestä asioinnista viranomaistoiminnassa 1 luku 1 §
http://www.finlex.fi/fi/laki/ajantasa/2003/20030013

5 TIETOTURVALLISUUS KUNNALLISHALLINNOSSA

Kuten jo aiemmin käsittelemässäni kohdassa lainsäädäntö ja tietoturvallisuus, tulee kunnallishallinnon tietoturvaa suunniteltaessa, toteutettaessa ja kehitettäessä ottaa huomioon useissa eri laissa määriteltyjä asioita.

Kunnallishallinnossa käsitellään tärkeää tietoa, kuten henkilöstötietoja, taloustietoja, erilaisia asiakirjoja ynnä muuta tietoa, joka voi olla salassa pidettävää, luottamuksellista tai muuten arkaluonteista.

Pienissä kunnissa ja kaupungeissa on usein tietoturvaan liittyvien asioiden kehittäminen, arviointi ja seuranta jäänyt puutteelliseksi johtuen usein henkilöstöresursseista, johdon tiedonpuutteesta tai välinpitämättömästä suhtautumisesta asiaan. Jos asiat ovat hoituneet hyvin tähänkin saakka eikä mitään isompia tietoturvaan liittyviä ongelmia ole sattunut, ei ole ollut mitään tarvetta miettiä tietoturvallisuuteen liittyviä riskejä.

Riippuvuus tietojärjestelmistä on tehnyt hallinnosta erittäin haavoittuvan turvallisuutta uhkaaville tekijöille. Lisäksi hallinnon ja yksityisten verkkojen yhdistäminen sekä palveluiden ulkoistaminen ovat heikentäneet virastojen mahdollisuuksia tehokkaaseen tietoturvallisuuden valvontaan. (VAHTI 7/2003, 5)

5.1 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmän mallin mukaan tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat ajantasainen tietoturvapolitiikka ja siihen liittyvät asiakirjat sekä säännöllinen riskienhallinta. Riskienhallinta koskee sekä nykyistä toimintaa että suunniteltuja muutoksia. Niiden pohjalta luodaan tietoturvastrategia ja suunnitelmat, joiden avulla tietoturvaratkaisut toteutetaan tietoturvavaatimusten mukaisesti. Hallintajärjestelmä sisältää myös tietoturvatoiminnan tehokkuuden ja tarkoituksenmukaisuuden säännöllisen mittaamisen ja arvioinnin. (VAHTI X/2007, 36)

6 YHTEENVETO

Kunnan tietoturvan suunnittelu ja kehittäminen pohjautuu kunnan johdon tekemiin periaatepäätöksiin ja ohjeistukseen. Organisaation hyväksymässä tietoturvapolitiikassa määritellään säännökset, joissa kerrotaan, mitkä asiat ovat sallittuja ja mitkä eivät. Myös vastuiden määritteleminen ja toimenpiteet rikkomusten tapahtuessa dokumentoidaan.

6.1 Lapinlahden kunnan tietoturvasuunnitelman toteuttaminen

Tietoturvasuunnitelman tarkoituksena oli Lapinlahden kunnan tietoturvan kehittämisen, ylläpidon ja seurannan toteutus niin, että se vastaa tietoturvasta sille asetettuja vaatimuksia. Tietoturvan tulee olla osana kunnan jokapäiväistä toimintaa.

Tietoturvallisuuden suunnittelu ja toteuttaminen vaati useiden eri asioiden läpi käymistä. Säännöksiä ja ohjeita on osattava hakea ja yhdistellä niitä oikein. Tietoturvallisuus käsitteenä on laaja aihealue ja tarkkaa ohjeistusta tai mallia ei kunnallishallintoon suoraan löytynyt. Oheistus oli suunniteltu pääsääntöisesti valtionhallinnon ja yritysten käyttöön.

Työn suunnittelu alkoi tutustumalla aihetta käsitteleviin julkaisuihin, joita löytyi paljon muun muassa valtiovarainministeriön sivuilta ja yritysten tietoturvaa käsittelevistä julkaisuista. Kuntien tietoturvaan liittyvän lainsäädännön etsiminen ja tarkastelu vei paljon aikaa. Samalla kuitenkin alkoi hahmottua tietoturvan suunnittelun pääpiirteet. Tietoturvaan liittyvien käsitteiden ja määritelmien ymmärtäminen oli perustana työn eteenpäin viemiseksi. Kunnan tietoturvan suunnittelulle oli hyvänä pohjana myös organisaation toimintatapojen tunteminen.

Kesällä 2011 työntekijöiden tietoturvaa testattiin tietoturvallisuuden perustason testillä, joka on liitteenä 1 olevassa taulukossa. Testiin kuului 20 kysymystä. Testi lähetettiin 20 henkilölle ja vastauksia tuli 14 henkilöltä. Virheellisiä vastauksia löytyi muun muassa tietoaineiston tietoturvallisesta käsittelystä, salassa pidettävien asiakirjojen luokittelusta, etäkäytöstä ja etätyöstä sekä muun sähköpostijärjestelmän kuin virkasähköpostin käyttämisestä omassa työssä. Liitteenä 2 oleva taulukko testituloksista on salainen.

Lapinlahden kunnalla ei ole tämän asiakirjan luomishetkellä erillistä tietoturvastrategiaa.

Kunnan virasto-organisaation keskeinen yksikkö on hallintokeskus, jonka tehtäviin kuuluu muun muassa posti-, puhelin- sekä perustietotekniikan palvelut. Tietotekniikan palvelujen kehittäminen ja ylläpito on ulkoistettu ja siitä vastaava yritys huolehtii perustietotekniikan sekä tele- ja mobiiliratkaisujen toimivuudesta, tietoturvasta, prosesseista ja tekniikan ajanmukaisuudesta. Sopimuksen mukaan palveluun kuuluvat työasemat, tulostimet, palvelimet ja tietoliikenne sekä erilaisia tietotekniikan ohjelmistoja laiteympäristöineen. Kaikkien palvelimien sekä tietoliikenteen laitteille annetaan palvelua kellon ympäri kaikkina päivinä. Tietoturvan hallinnasta vastaa kunnassa hallintojohtaja ja hänen varalla on kunnanjohtaja.

Kunnan tietohallinnan riskienhallintaa ei ole koordinoitu eikä keskitetty. Poikkeusolojen toimintojen turvaamista varten tehtyä valmiussuunnitelmaa päivitetään ja sen on tarkoitus valmistua vuoden 2011 loppuun mennessä. Asiakirjahallinnansuunnitelmaa päivitetään parhaillaan. Asiakirjahallinnan toimintaohjeet liitteineen ovat käytössä. Kunnan tietoturvasta löytyy ohjeistusta taloudenhoitoa ym. täydentävistä ohjeista sekä ulkoisen palveluntuottajan laatimista tietoturvaohjeista.

Kunnan johtoryhmä on tehnyt riskianalyysejä tietoturvaan liittyvistä asioista vuoden 2011 alkupuolella. Tietohallintariskeistä on tehty listauksia ja riskien vähentämisen ja pienentämisen ensisijaisia toimintatapoja on dokumentoitu. Keinoja riskien vähentämiseen ja pienentämiseen on tehty kaikista käsitellyistä tietohallinnan riskeistä. Tietoturvatoiminnan tuloksista raportoidaan ja seurannan aikataulu laaditaan. Kehittämistarpeet tietoturvallisuuden lisäämiseksi kohdistuvat tiedottamiseen, perehdyttämiseen ja tietoturvakoulutukseen.

6.2. Lopputulokset

Työn tekeminen on ollut sekä haasteellista että antoisaa. Tietoturvallisuuteen suhtautuminen on saanut uusia piirteitä. Tiedon hakeminen ja dokumentointi on kehittynyt työn edetessä. Työn tekemiseen tarvittavia tietoja ei ollut saatavilla niin paljon, kuin suunnitelman yksityiskohtaiseen esittelemiseen olisi tarvittu. Opinnäytetyön tuloksena syntynyt Lapinlahden kunnan hallinnon ensimmäinen tietoturvasuunnitelma on tieto-

turvan kehittämiseen suunniteltu, suuntaa antava dokumentti, jota päivitetään jatkossa tarpeen mukaan.

Lopuksi haluan painottaa sitä, ettei pienissä kunnissa ole useinkaan mahdollista ylläpitää omia tietotekniikan yksiköitä, jotka tuottavat ja turvaavat tietoteknisiä palveluja, koska palvelut vaativat suuria henkilöstöresursseja ja asiantuntemusta. Tämän vuoksi palveluja ostetaan tietopalveluyrityksiltä ja kyseessä on usein sekä kustannus- että osaamiskysymys. Tietotekniikan nopea kasvaminen ja uusien asioiden hallinta vaatii asiantuntijuuden ja erikoistumisen turvaamista.

Kun tietotekniikan palveluja ulkoistetaan, jää kunnille itselleen harvoin enää erillistä tietotekniikan asiantuntijaa, joka huolehtisi palvelujen tilaamisesta ja asioiden priorisoinnista. Tähän ongelmaan tulisi mielestäni suhtautua kriittisesti ja miettiä osaamisen säilymistä omassa organisaatiossa.

Lapinlahden kunnan hallinnon tietoturvasuunnitelma on salainen ja se on liitteenä 3.

LÄHTEET

Finlex. (2012). *Arkistolaki*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1994/19940831

Finlex. (2012). *Henkilötietolaki*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Finlex. (2012). *Laki sähköisestä asioinnista viranomaistoiminnassa*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2003/20030013

Finlex. (2012). *Laki viranomaisten toiminnan julkisuudesta*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Finlex. (2012). *Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/alkup/1999/19990565

Finlex. (2012). *Rikoslaki*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Finlex. (2012). *Suomen perustuslaki*. Haettu 17. toukokuu 2012 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Kunnat.net. (2011). *Tietoturva*. Haettu 3. Lokakuu 2011 osoitteesta http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/tietohallinto/tietoturva/Sivut/default.aspx

PK-RH. (2011). *Pk-Yrityksen riskienhallinta*. Haettu 3. Lokakuu 2011 osoitteesta http://www.pk-rh.fi/startti-riskienhallintaan/mita-riskienhallinta-on/riskienhallintaprosessin-vaiheet/

Tietoturvaopas. (2003). *Testaa tietosi*. Haettu 17. toukokuu 2012 osoitteesta http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/testi_k/20kysym.htm

Valtiovarainministeriö. (2011). *Käyttäjän tietoturvaohje 5/2003*. Haettu 3. Lokakuu 2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf

Valtiovarainministeriö. (2003). *Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa*. Haettu 3. Lokakuu 2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf

Valtiovarainministeriö. (2007). *Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan*. Haettu 3. Lokakuu 2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070619Lausun_15158/02_Yleisohje_20070619_4_.pdf

Viestintävirasto. (2009). *Tietoturva- ja suoja*. Haettu 3. Lokakuu 2011 osoitteesta http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

LIITTEET

Liite 1 Tietoturvallisuuden perustason testi

Tietoturvallisuuden perustason testi löytyy Tietoturvaopas-sivustolta (kaikille julkishallinnon käyttäjille tarkoitettu tietoturvaopas). Kyselyssä on 20 kysymystä, jotka mittaavat tietoa kattavasti tietoturvan eri osa-alueilta. Seuraavassa testin kysymykset vastausvaihtoehtoineen niin kuin ne testissä esitetään:

Testaa tietosi: 20 kysymystä tietoturvallisuudesta

Tietoturvallisuuden perustason testi

1. Mikä on julkishallinnon tietoturvallisuuden perusta?
   - Standardeihin
   - Lainsäädäntöön ja normiohjaukseen
   - Ns. hyviin käytäntöihin (best practices)

2. Minkä tiedon ominaisuuden määritelmä on "tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja eikä muutoin käsitellä tietoja."?
   - Luottamuksellisuus
   - Eheys
   - Käytettävyys

3. Mikä seuraavista vaikuttaa tietoaineiston tietoturvalliseen käsittelyyn?
   - Tiedon elinkaaren vaihe
   - Aineiston luokittelu
   - Käsittelijän työtehtävä

4. Kuka vastaa salassa pidettävän asiakirjan luokittelusta ja merkinnästä?
   - Organisaatiossa erikseen nimetty, luokittelusta vastaava(t) henkilö(t)
   - Tietoturvavastaava
   - Asiakirjan laatija tehtäviensä mukaisesti

5. Mitä seuraavista ei tarvitse tehdä salassa pidettävää aineistoa

lähetettäessä?

- Vastaanottajan tietojen tarkistaminen ja varmistus, että vastaanottaja on oikeutettu saamaan salassa pidettävää aineistoa
- Aineiston luokituksen merkitseminen
- Ilmoitus esimiehelle lähetyksestä
-

6. Miten salassa pidettävä aineisto hävitetään?

- Laittamalla se tiedon suojausvaatimusten mukaisiin tietoturva-aineiston keräyslaatikoihin tai silppuriin
- Antamalla se suoraan siivoojalle hävitettäväksi
- Samalla tavoin kuin muukin hävitettävä aineisto

7. Mitä vaaditaan etäkäyttöön ja etätyöhön?

- Riittävän laajat käyttöoikeudet
- Esimiehen lupa
- Sopimus

8. Miksi kaikkea virastossa tehtävää ei voi tehdä etätyönä?

- Työssä tarvittava tieto- ja aineistomäärä on liian suuri käsiteltäväksi etätyössä.
- Aineiston luokittelu ja siihen liittyvä käyttö sekä luovutusta, käyttöä ja käsittelyä koskevat rajoitukset on otettava huomioon etätyössäkin.
- Laajamittaiseen etäkäyttöön tarvittavat laitteet ja ohjelmistot ovat liian kalliita hankkia.

9. Mitä tarkoittaa "Puhtaan pöydän -periaate"?

- Työpöydällä ei säilytetä salassa pidettävää aineistoa.
- Työpöydällä ei säilytetä mitään työaineistoa.
- Työpöydällä oleva aineisto on oltava hyvässä järjestyksessä.

10. Työntekijän vaitiolovelvollisuus koskee mm. hänen tietoonsa tulleita yksityisiä viestejä. Mikä muu alla olevista kuuluu vaitiolovelvollisuuden piiriin?

- Toiselle henkilölle tarkoitetut, vahingossa väärään osoitteeseen tulleet sähköpostiviestit
- Mahdolliset haittaohjelmaepäilyt (virukset, madot, troijalaiset)
- Toimitiloissa liikkuvat epäilyttävät tai tuntemattomat henkilöt.

11. Minkä perusteella tietojärjestelmien käyttöoikeudet annetaan?

- Käyttäjän toiveen perusteella
- Käyttäjän työtehtävän perusteella
- Lainsäädännön perusteella

12. Kenelle saa tarvittaessa luovuttaa henkilökohtaiset käyttöoikeudet ja salasanat?
    - Atk-henkilöstölle
    - Sihteerille
    - Ei kenellekään

13. Kuka saa asentaa ja päivittää ohjelmia ja laitteita?
    - Tietohallinto
    - Asiantunteva työkaveri tai perheenjäsen
    - Käyttäjä itse

14. Mihin tietovarastojen tietoja saa käyttää?
    - Tietovarastojen käytöllä ei ole rajoituksia
    - Yleisesti kaikkiin organisaation tehtäviin
    - Vain omiin työ-/virkatehtäviin

15. Jos käytät julkisia päätteitä tai toisen henkilön tietokonetta, niin mitä sinun ei tarvitse tehdä lopetettuasi työskentelyn?
    - Vaihtaa salasanasi
    - Kirjautua ulos ohjelmistosta ja koneelta
    - Tyhjentää Internet-selaimen välimuisti ja evästeet

16. Mikä näistä on hyvä salasana?
    - monitori
    - maija1968
    - Tes9753Ti03

17. Milloin täytyy käyttää salausta, kun lähetetään tietoa Internetin kautta?
    - Aina
    - Kun tieto on salassa pidettävää
    - Oman harkinnan mukaisesti

18. Mitä täytyy tehdä, jos saa sähköpostissa roskapostia?

- Tuhota viestit välittömästi
- Välittää viestit atk-henkilöstölle
- Vastata ja pyytää, ettei postia enää lähetettäisi

19. Missä virkasähköpostia **ei** saa käsitellä?
    - Omilla yksityisillä laitteilla ja ohjelmistoilla
    - Oman organisaation laitteilla ja ohjelmistoilla
    - Muun julkishallinnon organisaation laitteilla ja ohjelmistoilla

20. Missä tilanteessa töissä voi käyttää muuta sähköpostijärjestelmää tai -osoitetta kuin virkasähköpostia?
    - Ei koskaan
    - Silloin, kun siihen on oman organisaation lupa
    - Silloin, kun virkasähköposti ei toimi

    lähde: Tietoturvaopas. [viitattu 3.8.2011].
    http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/testi_k/20kysym.htm